AMA
AMERICAN MEDICAL ASSOCIATION

James L. Madara, MD
CEO, EXECUTIVE VICE PRESIDENT

james.madara@ama-assn.org

May 25, 2022

Lisa J. Pino
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: HITECH Act Recognized Security Practices Request for Information, RIN 0945-AA04

Dear Director Pino:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the Office for Civil Rights (OCR) Request for Information (RFI) on certain provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Public Law 116-321

The AMA wholeheartedly supports OCR's interest in providing information to regulated entities that helps them understand the application of Public Law 116-321 (Section 13412 of the HITECH Act), which provides that OCR consider recognized security practices of covered entities and business associates when making determinations regarding fines, audits, and remedies to resolve potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.[1] The AMA advocated for such a policy and believes OCR's urgent attention to this matter is critical to the health care sector's resilience against increasing threats of cyber attacks.

We strongly urge OCR to coordinate with the National Institute of Science and Technology (NIST). NIST has developed valuable resources that provide guidance on cybersecurity trends and recommend best practices to individuals and organizations across the country, including many physician practices. NIST recognizes that cybersecurity practices will vary across organizations, depending on levels of technical understanding, financial and human resources, and risk tolerance. This flexibility allows entities to customize how they adopt and implement a cybersecurity framework and is critical in the health care space where a solo practitioner has very different resources than a large health system. It also makes it difficult to answer OCR's question of which NIST resources regulated entities rely on when establishing and implementing recognized security practices.

[1] Pub. L. 116-321 (January 5, 2021). Available at https://www.congress.gov/bill/116th-congress/house-bill/7898.

We also highly recommend the resources promulgated under section 405(d) of the Cybersecurity Act of 2015.[2] The AMA has publicized these resources on its own cybersecurity page,[3] and is particularly grateful for its attention to providing resources for small physician practices. AMA members and the House of Medicine have expressed increased concerns over cybersecurity in recent years, and the 405(d) resources have been timely, informative, and user-friendly. Additionally, the U.S. Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) recently launched a new website to help physicians and their medical practices be better informed about potential cyber threats.[4] This new site lists several resources, including threat briefs with best practices and information on COVID-19 related cyber threats and sector alerts with high-level information to assist non-technical audiences. We also often refer physicians to the website of the Healthcare and Public Health Sector Coordinating Council Cybersecurity Working Group, which is comprised of experts across the health care sector, many of whom are actively monitoring health care threats and trends particularly relevant to the field.[5] Lastly, the AMA encourages OCR to consider a physician's intent to implement the above recognized security practices with the understanding that many medical practices have limited resources. Evaluating adequate demonstration of recognized security practices should be done in the context of a covered entity's practice size, geographic location, and access to staff with expertise in cybersecurity.

Section 13410(c)(3)

OCR seeks information on current real-world impacts of loss of privacy on an individual's willingness to seek care or disclose health information to covered entities. The AMA has long advocated for increased attention to how lack of privacy can negatively impact the patient-physician relationship.[6] We learn more each day that personal health information is no longer private. Social media platforms, wearable fitness trackers, and applications (apps) allowing patients to download health records from electronic health records and manage health conditions all collect data that are not protected by HIPAA. That means these data can be shared for a wide range of purposes, including advertising and marketing. Sharing that health information with data brokers, who can combine it with other consumer information (such as credit score, level of education, and even something as simple as a zip code), creates the perfect recipe for harmful profiling and discrimination.[7] Data mining by insurers and employers leads to the creation of health or "risk" scores, which can result in harmful profiling and discrimination. Social media platforms, Internet search engines, wearable fitness trackers, and apps to manage pregnancy and mental health all pool personal data, turning it into a valuable commodity. For example, a recent evaluation of the 23 most popular women's mobile health (mHealth) apps on the market has shown that all collect personal health-related data. All apps allowed behavioral tracking and over 60 percent allowed location tracking. Only 52 percent requested consent from users and 13 percent collected data before obtaining consent.[8] At a time when women's reproductive rights are in jeopardy, the fact that popular women's mHealth apps lack data privacy, sharing, and security standards is concerning.

[2] https://405d.hhs.gov/public/navigation/newsAndAwarenessResources

[3] https://www.ama-assn.org/practice-management/sustainability/physician-cybersecurity

[4] https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

[5] https://healthsectorcouncil.org/

[6] *See* e.g., https://www.ama-assn.org/delivering-care/patient-support-advocacy/patient-data-privacy-and-access-resources and https://www.ama-assn.org/delivering-care/patient-support-advocacy/ama-health-data-privacy-framework

[7] Favaretto, M., De Clercq, E. & Elger, B.S. Big Data and discrimination: perils, promises and solutions. A systematic review. *J Big Data* 6, 12 (2019). https://doi.org/10.1186/s40537-019-0177-4.

[8] Alfawzan N, Christen M, Spitale G, Biller-Andorno N Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis (May 2022), available at https://mhealth.jmir.org/2022/5/e33735

Indeed, there is growing awareness among patients of how companies monetize individuals' health and other personal information. A 2019 Morning Consult national survey showed that 94 percent of people feel privacy and security of their medical information are important,[9] while a 2019 study by Rock Health and Stanford's Center for Digital Health shows consumers have become more reticent to share their health data.[10] Among health care stakeholders, consumers are most willing to share their health data with physicians, but that sentiment has slipped since 2017, possibly due to spillover from privacy and security breaches in other sectors and general distrust of "big tech."[11] A 2017 Black Book survey reports that:

- 87 percent of patients were unwilling to comprehensively share all of their health information with their physicians;
- 89 percent of consumers who had visited a health care provider in 2016 said they had withheld some information during their visits;
- 81 percent were concerned that information about chronic conditions was being shared without their knowledge; and
- 99 percent were concerned about the sharing of mental health notes.[12]

New survey data from the AMA and Savvy Cooperative, a patient-owned co-op that connects people with opportunities to share their health experiences, found that nearly three-quarters of surveyed patients are concerned about the privacy of their health data. Additionally, 59 percent of patients are worried about health data being used by companies to discriminate against them or their loved ones or to exclude them from opportunities to find housing, gain employment, and receive benefits. Over half of surveyed patients stated that they are very or extremely concerned about negative repercussions related to insurance coverage, employment, or opportunities for health care resulting from access to their health data. When asked to indicate how comfortable they are with certain types of companies gaining access to their health data, survey patients were overwhelmingly most comfortable with their physician's office having such access. Conversely, patients were least comfortable with social media sites, employers, and big technology companies receiving access to their health data.

Together, these findings indicate that carelessness and lack of transparency in how patient information is handled and used by technology has likely influenced what information a patient shares with his or her physician. **This should serve as a warning to policymakers that patients take their health data privacy seriously and that privacy safeguards are critical to preserving patient trust.**[13] Whichever methodologies and practices OCR utilizes to implement Section 13410(c)(3), we urge it to be explicit about the policy contours with both regulated entities and patients. In other words, regulated entities

[9] Morning Consult National Tracking Poll (June 20-22, 2019), available at https://www.uschamber.com/sites/default/files/190645_topline_adults_v2_jb.pdf.

[10] Digital Health Consumer Adoption Report 2019, available at https://rockhealth.com/reports/digital-health-consumer-adoption-report-2019/.

[11] Sean Day and Megan Zweig, Rock Health, *Beyond Wellness for the Healthy: Digital Health Consumer Adoption 2018*, available at https://rockhealth.com/reports/beyond-wellness-for-the-healthy-digital-health-consumer-adoption-2018/.

[12] Black Book Market Research, *Healthcare's Digital Divide Widens* (Jan. 3, 2017), available at https://blackbookmarketresearch.newswire.com/news/healthcares-digital-divide-widens-black-book-consumer-survey-18432252.

[13] "Incomplete medical histories and undisclosed conditions, treatment or medications raises obvious concerns on the reliability and usefulness of patient health data in application of risk based analytics, care plans, modeling, payment reforms, and population health programming." Doug Brown, Black Book Managing Partner, available at https://www.prnewswire.com/news-releases/healthcares-digital-divide-widens-black-book-consumer-survey-300384816.html.

should be assured that OCR will not inadvertently incentivize unreasonable or frivolous complaints of breach due to patient misunderstanding of what HIPAA does and does not permit or, worse, targeted harassment of physicians out of hope of personal financial benefit. **We also stress that more must be done to help patients and physicians better understand the ramifications of health data being siphoned into health apps.** OCR should establish a national campaign to educate individuals about their rights to data and methods to help protect themselves from data misuse. Furthermore, OCR should provide targeted outreach and educational materials to regulated entities and patients explaining the process used to implement Section 13410(c)(3) and best practices to protect data. OCR should also consider and publicize what steps it will take to correct its formula should that become necessary. For example, OCR notes in the RFI that certain portions of funds are currently allocated to support enforcement action activity. OCR must ensure that if breach complaints increase and patients receive a portion of any assessed fines, OCR is able to continue conducting more investigations with fewer financial resources. Patient trust will deteriorate if patients cannot trust that OCR has the resources and bandwidth to adequately investigate and enforce their reports of breach.

We appreciate the opportunity to provide this information and look forward to continued conversations surrounding this important issue. If you have any questions, please contact Matt Reid, Senior Health IT Consultant, at matt.reid@ama-assn.org.

Sincerely,

James L. Madara, MD